UDC 623.1/.3:351.746:656.7 https://doi.org/10.33099/2304-2745/2026-1-87/32-39

Akhundov R., PhD (National Security and Military)[1] (0009-0001-8798-8044)
Hashimov E. Г.[2], DsM, professor[2] (0000-0001-8783-1277)
Chelobitchenko A. A., PhD (Technical), senior researcher[3] (0000-0002-9411-2569)

[1] – National Defence University of Azerbaijan, Baku, Azerbaijan;
[2] – Azerbaijan Technical University, Baku, Azerbaijan;
[3] – State Research Institute of Aviation, Kyiv, Ukraine

Information-to-Action Requirements for Airbase Physical Protection Under High-Tempo Operations

Resume. The study addresses information processes in the physical protection of airbases and airfields operating under high-tempo conditions, where dense legitimate activity increases ambiguity and produces heavy alarm load. The paper focuses on information-to-action performance as a sufficiency-critical factor that links sensing to validated decisions, dispatch, and response activation within a time window that enables interruption before the adversary reaches a critical element. The aim is to derive measurable information-to-action requirements for aviation facilities that remain defensible under concurrency, false-alarm surges, degraded communications, and insider-assisted conditions. The methodology combines a bounded scenario library with a latency decomposition into $t_{det}, t_{val}, t_{fus}, t_{dec}, t_{com}, t_{disp}$, bottleneck identification per scenario class, and requirement derivation as time bounds and quality targets.

The framework is applicable to conceptual design, procurement specifications for SOC and C2 workflows, acceptance testing programs, and lifecycle revalidation using operational logs and after-action review.

Keywords: airbase security; physical protection system; information-to-action latency; alarm validation, decision latency; command and control; communications resilience; scenario-based requirements; acceptance evidence.

Problem Statement. Airbases and other aviation facilities operate as high-tempo socio-technical systems in which continuous movements of aircraft, vehicles, personnel, and contractors generate a dense background of legitimate activity. This operational density increases the attack surface and complicates the discrimination of threat-relevant signals from routine events. At the same time, the protected assets are high-consequence by nature, including aircraft on aprons, hardened shelters and hangars, fuel farms, ammunition and explosives storage, air traffic control and command-and-control nodes, and power and communications infrastructure. In such environments, physical protection performance is determined not only by sensors, barriers, and patrol patterns, but by the speed and reliability with which heterogeneous information is converted into validated decisions and timely dispatch. Under surge operations, concurrent disturbances, or communications degradation, even a technically well-instrumented perimeter can become operationally insufficient if the information-to-action loop cannot preserve the time reserve needed for interruption.

The problem addressed in this paper is that conceptual physical protection design for airbases often remains measure-centric and implicitly assumes near-perfect information, negligible validation time, and stable communications. In practice, the most consequential delays frequently occur after the initial alarm, during validation, fusion, decision authorization, and dissemination. High false-alarm load, ambiguity in sensor signals, operator workload, competing operational priorities, and degraded communications can expand information-to-action time to the point where the integrated detection–delay–response chain no longer satisfies scenario-conditioned sufficiency. This creates a defensibility gap in design review: compliance can be documented while the system remains unable to guarantee timely intervention under representative adversarial scenarios, including coordinated diversion, insider-enabled access, and multi-event saturation. The operational and defense relevance of this problem is direct, because aviation facilities must maintain continuity of sortie generation and command functions while remaining resilient to time-compressed attacks and rapid escalation.

Analysis of Recent Research and Publications. Prior research has examined key elements of this challenge, but typically in fragmented form. The detection–delay–response paradigm and time-conditioned interruption logic are well established in the physical protection literature and provide a baseline for

sufficiency reasoning [1–4]. Scenario-based requirement setting and risk-informed design methods have been proposed to improve relevance under adaptive threats and to support differentiated protection across zones and assets [5–7]. Studies on security operations centers, alarm management, situation awareness, and decision latency show that validation and decision stages can dominate defender timelines under uncertainty and workload, particularly in high-noise operating environments [8–11]. Work on multi-source fusion, video analytics, access-control correlation, and communications resilience indicates that improvements in information quality can enhance classification and prioritization, but may also introduce processing latency if workflows and escalation rules are not engineered explicitly [12–15]. For aviation facilities, layered security and access control are widely emphasized, yet the literature rarely provides a unified method for deriving measurable information-to-action requirements that remain valid under high-tempo operations, concurrency, and degraded communications [16–18, 31]. As a result, a methodological gap persists between threat characterization and design requirements that can be verified with defensible acceptance evidence.

The aim of this article is to formalize an information-to-action requirement framework for airbase physical protection under high-tempo operations by translating representative airbase scenarios into measurable latency and information-quality targets with explicit acceptance evidence. Specifically, the paper (I) defines an airbase-relevant scenario set that stresses distinct information bottlenecks, (II) decomposes information-to-action time into operational stages $t_{\mathrm{det}}, t_{\mathrm{val}}, t_{\mathrm{fus}}, t_{\mathrm{dec}}, t_{\mathrm{com}}, t_{\mathrm{disp}}$, (III) derives requirement templates that bound these components and specify minimum quality thresholds (for example timely detection and classification performance) under nominal and degraded conditions, and (IV) links each requirement to predefined verification pathways using instrumented drills, log-based measurement, stress testing, and simulation or hybrid evidence when empirical sampling is limited. The intended contribution is a review-defensible bridge from airbase threat mechanisms to verifiable information requirements that can support conceptual design, procurement, testing, and lifecycle revalidation.

Main material. Airbase physical protection must be treated as a high-tempo socio-technical control system in which the decisive variable is not the nominal presence of sensors or barriers, but the ability to convert heterogeneous signals into a validated decision and a dispatched response before an adversary reaches the critical element [19, 20]. In aviation settings, the operational environment is inherently noisy. Aircraft turnarounds, ground support equipment, scheduled and unscheduled vehicle movements, contractor access, and transient workforce flows generate a large volume of legitimate events that are, from the perspective of a security operations center, statistically similar to low-signature hostile preparation [21–24]. This is precisely why information processes must be engineered and justified at the conceptual stage. If information-to-action performance is not specified as a measurable requirement, the design will drift toward hardware-centric compliance while the operational bottleneck remains in validation, decision, and communications under overload.

A practical conceptual model begins with an explicit definition of protected assets and critical elements in airbase topology. While perimeter integrity remains necessary, it is rarely sufficient as a design focus because many high-consequence targets are located deep within the installation and are connected by predictable movement corridors. For requirement justification, the facility should be represented as a set of functional zones and transitions that reflect both operational use and threat-relevant access: perimeter and controlled entry points, flight line and apron areas, hardened shelters and hangars, fuel farms and distribution nodes, ammunition storage and handling zones, air traffic control and command-and-control nodes, and the power and communications backbone that enables sortie generation [25-30]. The key conceptual decision is to define which critical elements constitute unacceptable consequence endpoints for each scenario class and to specify the allowable time window for intervention before those endpoints are reached. This is the point at which “information-to-action” requirements become non-negotiable because they determine whether the defender can exploit any delay capacity created by the physical layer.

The scenario model for airbases should be bounded but representative, emphasizing distinct failure mechanisms rather than superficial variations. A minimal library typically includes covert intrusion toward a high-value apron or hangar, forced entry through a gate or fence segment, targeted

sabotage of fuel or communications nodes, diversion plus main attack that saturates response, insider-assisted access through credentials or escort abuse, coordinated multi-point activity that overloads command and control, and incidents involving small unmanned aerial systems that generate both threat exposure and alarm noise. Each scenario should be specified with an operating state that reflects airbase reality, such as routine tempo, surge operations, degraded communications, heightened alert posture, and staffing constraints. The purpose of scenario definition here is methodological: it establishes which information bottleneck is expected to dominate, and therefore which information requirement must be bounded to preserve sufficiency.

Information-to-action performance is formalized through a latency decomposition that makes post-detection delays explicit and measurable. For a scenario s, total information-to-action time is defined as

$$T_{info}(s) = t_{det}(s) + t_{val}(s) + t_{fus}(s) + t_{dec}(s) + t_{com}(s) + t_{disp}(s),$$

where detection latency t_{det} covers event onset to first system indication, validation t_{val} covers acknowledgement and confirmation, fusion t_{fus} covers multi-source correlation if used, decision t_{dec}covers classification and authorization, communications t_{com} covers dissemination to responders, and dispatch t_{disp} covers mobilization.

This decomposition is not an accounting exercise; it is the conceptual bridge between information processes and the classical detection–delay–response chain. In interruption logic, defender time to effective intervention includes both information processing and physical response execution. A compact representation is

$$T_D(s) = T_{\mathrm{info}}(s) + t_{\mathrm{travel}}(s) + t_{\mathrm{eng}}(s),$$

and sufficiency is preserved only if $T_D(s)$remains below adversary time to target $T_A(s)$with a defined margin. Consequently, conceptual requirements must explicitly bound the information portion of the defender chain, not only the travel and engagement portions.

Airbase-specific stressors make uncertainty and overload essential parts of the model rather than optional refinements. High false-alarm rate and ambiguous detections increase $t_{\mathrm{val}}$and t_{dec}through operator workload and queueing. Communications degradation increases $t_{\mathrm{com}}$and can cause partial delivery failure that forces re-verification, indirectly increasing validation and decision time. Insider-assisted actions reduce the discriminatory power of perimeter sensors and shift the burden to access-control correlation and anomaly detection, which may increase fusion and validation time unless the workflow is engineered for rapid escalation. For these reasons, information requirements should be expressed not only as nominal bounds but also as degraded-mode targets, and when evidence allows, through probabilistic acceptance forms. A defensible conceptual option is to require that a latency bound holds with an explicit risk tolerance, for example $\Pr\big(T_{\mathrm{info}}(s) \le \bar{T}_{\mathrm{info}}(s)\big) \ge 1 - \varepsilon_s$, particularly for concurrency and diversion scenarios where overload is the main failure mechanism.

Deriving requirements from scenarios should follow a consistent template: identify the dominant bottleneck for each scenario class, then bound the time components and quality metrics that control that bottleneck, and finally specify acceptance evidence that can be collected in operations. For covert intrusion, the binding risk is late confirmation under weak signatures; the conceptual requirement is therefore a strict bound on validation and decision time and a minimum timely detection and classification capability. For forced entry, the first signal is usually strong, but the time window is short; the requirement concentrates on detection latency and rapid dispatch, supported by resilient communications. For diversion plus main attack, the issue is not single-event performance but queue stability under multi-event load; requirements must include alarm load tolerance, prioritization rules, and acceptance evidence under concurrent injections. For insider-assisted access, requirements focus on correlation of access-control events with spatial anomalies and rapid escalation without excessive manual verification. For communications degradation, the conceptual requirement is a minimum communications availability and bounded message latency in degraded mode, plus fallback procedures that prevent decision deadlocks. At this point in the manuscript, a scenario matrix is necessary to keep the derivation auditable and to show coverage of failure mechanisms.

Table 1 is included at this point to consolidate the scenario classes analyzed for airbase protection, to map each class to its

dominant information-process bottleneck, and to indicate the primary evidence channel used for acceptance.

Table 1 summarizes the airbase scenario classes considered in the study, highlights the dominant information bottleneck in each class, and indicates the primary acceptance evidence channel used for verification.

The measurable content of information requirements must include both latency and quality. Latency targets alone can produce brittle automation that is fast but wrong; quality targets alone can produce systems that are accurate but too slow.

Table 1

Airbase scenario matrix: dominant information bottlenecks and acceptance evidence (Source: developed by the authors)

Scenario class	Typical target and zone	Operating state (θ)	Dominant information bottleneck	Key information-to-action requirement focus	Preferred acceptance evidence
Covert intrusion to flightline	Aircraft parking, apron, hangar access points	Routine plus night operations, high background movement	Late confirmation under weak signatures, growth of $t_{\mathrm{val}} + t_{\mathrm{dec}}$	Tight bounds on t_{val}, t_{dec}; minimum P_D and P_C for low-signature patterns	Instrumented drills with low-signature injects; labeled analytics evaluation; log-based latency measurement
Forced entry at gate or fence segment	Perimeter, gate, service road entry	Surge operations, vehicle queues, mixed access	Fast escalation window, sensitivity to $t_{\mathrm{det}} + t_{\mathrm{disp}}$	Bound t_{det}, t_{com}, t_{disp}; ensure dispatch speed under noise	Timed gate-breach exercises; dispatch logs; comms delivery tests
Targeted sabotage of fuel node	Fuel farm, hydrant nodes, distribution control	Routine plus degraded staffing	Ambiguity of early indicators, delayed escalation, high impact of t_{dec}	Bound t_{dec} and escalation path; strengthen classification P_C for fuel-node anomalies	Red-team drills; access-control correlation tests; after-action log analysis
Diversion plus main attack	Diversion near perimeter plus main path to critical element	High tempo, concurrent incidents	Queue overload, prioritization failure, unstable t_{val} and t_{dec} under load	Workload tolerance, bounded $t_{\mathrm{val}} + t_{\mathrm{dec}}$ under concurrency; probabilistic acceptance for T_{info}	Multi-event exercises; alarm-injection stress tests; simulation or hybrid evidence for concurrency tails
Insider-assisted access	Restricted internal zones, maintenance areas, C2 nodes	Routine plus contractor surge	Boundary collapse, reliance on correlation, log integrity; delayed anomaly validation	Strong P_C for credential misuse; low t_{val} for access anomalies; integrity of logs	Access-control audits; targeted insider scenario drills; forensic log validation
Coordinated multi-point activity	Multiple gates or multiple internal nodes	Heightened alert, parallel events	C2 overload, communications congestion, growth of t_{com} and t_{dec}	Bound t_{com}, t_{dec} under concurrency; ensure A_{com} in stress mode	Coordinated drills; C2 workload tests; comms stress tests
Communications degradation during incident	Any critical element; emphasis on dispatch chain	Degraded comms, partial network loss	Increased t_{com}, message loss, repeated validation cycles	Availability target A_{com}, loss target L_{loss}, bounded t_{com} in degraded mode	Degraded-mode exercises; network telemetry; controlled comms degradation tests
Small UAS event with alarm noise	Flightline perimeter, approach corridors	High tempo, frequent nuisance detections	False-alarm surge, validation delay, operator fatigue	FAR limits, queue stability, bounded t_{val} as function of workload	Log-based measurement; controlled alarm injections; operator workflow evaluation

Therefore, requirements should combine bounds on $t_{\mathrm{det}}, t_{\mathrm{val}}, t_{\mathrm{dec}}, t_{\mathrm{com}}, t_{\mathrm{disp}}$ with minimum thresholds on timely detection probability, classification accuracy, false-alarm rate, and communications availability. A compact metric catalogue is essential for implementation and review. Table 2 is provided here to catalogue the information-to-action metrics used in the study, specifying for each metric its operational definition, primary data source, and the corresponding acceptance target form. In airbase settings, the measurement source is not an afterthought. If time stamps are inconsistent across sensor logs, SOC events, dispatch records, and communications telemetry, the organization cannot credibly claim that information-to-action requirements are satisfied. Thus, the conceptual design must include minimal logging and time

synchronization requirements as enabling constraints.

Table 2 lists the information-to-action metrics applied in the framework, providing each metric's definition, main data source, and the template form of the acceptance target.

Verification and acceptance evidence should be defined as part of the requirement object, because information performance is only defensible when it is measurable under controlled conditions.

The evidence strategy for airbases should combine instrumented timed drills, log-based measurement during routine and surge operations, stress tests that inject alarm load or degrade communications, and simulation or hybrid evidence for rare-event concurrency that is expensive to reproduce empirically. Instrumented drills are best suited for measuring $t_{\mathrm{val}}, t_{\mathrm{dec}}, t_{\mathrm{disp}}$ under standardized playbooks, while log-based measurement is necessary to validate that performance persists in real operational tempo. Stress tests are necessary to validate overload resilience, because average performance in quiet periods is not relevant to diversion scenarios. Simulation should not replace measurement but can support acceptance for probability-based claims, provided that assumptions are transparent and calibrated against observed data.

Table 2

Information-to-action metric set for airbase PPS design

(Source: developed by the authors)

Metric	Definition	Primary data source	Target type
t_{det}	Detection latency from event onset to first system indication	Sensor timestamps; event correlation logs	Upper bound (time)
t_{val}	Validation time from first indication to confirmed event status	SOC logs; operator acknowledgement records	Upper bound (time)
t_{fus}	Fusion time to consolidate multi-source inputs into one event hypothesis	Fusion engine logs; analytics pipeline logs	Upper bound (time)
t_{dec}	Decision and authorization latency to select and approve an action	C2 decision logs; escalation records	Upper bound (time)
t_{com}	Communications latency for delivering directives and context to responders	Network telemetry; message delivery receipts	Upper bound (time)
$t_{dısp}$	Dispatch and mobilization time from decision to response activation	Dispatch logs; unit status logs	Upper bound (time)
$T_{ınfo}$	Total information-to-action time $t_{\mathrm{det}} + t_{\mathrm{val}} + t_{\mathrm{fus}} + t_{\mathrm{dec}} + t_{\mathrm{com}} + t_{\mathrm{disp}}$	Integrated SOC and C2 logs	Upper bound (time) / Probabilistic bound (optional)
P_D	Probability of timely detection within specified window	Test campaigns; labeled data; validated simulation	Lower bound (probability)
P_C	Probability of correct classification (threat vs nuisance, scenario label)	Labeled datasets; red-team drills; analytics QA	Lower bound (probability)
FAR	False alarm rate per zone per unit time	SOC alarm logs; analytics outputs	Upper bound (rate)
A_{com}	Communications availability, successful delivery ratio	Network monitoring; delivery receipts	Lower bound (availability)
L_{loss}	Message loss rate under nominal and degraded conditions	Network telemetry; stress tests	Upper bound (rate)
W	Workload indicator, alerts per minute or queue length in SOC	SOC dashboards; ticketing queues	Upper bound (workload)
Δ_{clk}	Time synchronization error across systems (sensors, SOC, C2)	NTP/PTP monitoring; audit logs	Upper bound (time)
ε_s	Risk tolerance for probabilistic acceptance	Governance parameter	Governance parameter (risk tolerance)

The principal practical output of this section is a defensible conceptual method to set information-to-action requirements for airbases in a way that is compatible with sufficiency arguments. The contribution is not merely to list metrics, but to establish a repeatable derivation logic: scenario definition identifies bottlenecks, bottlenecks determine which latency and quality metrics must be bounded, and those bounds are paired with explicit evidence pathways. This creates a design review artifact that is both operationally meaningful and auditable. It also enables lifecycle revalidation. As airbase tempo, technology, staffing, and threat behavior evolve, the same structure can be used to re-estimate T_{info}, identify drift in validation and decision latency, and update thresholds without losing traceability to the scenario justification.

Conclusions. The study addresses a defense-relevant scientific and practical problem by justifying physical protection requirements for airbases and airfields under high-tempo

operations. It is shown that operational sufficiency in aviation facilities is determined not only by the presence of sensors and physical barriers, but by the performance of the information-to-action loop that creates the usable time reserve for interruption.

A self-contained methodological result is provided in the form of a measurable information–time model decomposed into $t_{\text{det}}, t_{\text{val}}, t_{\text{fus}}, t_{\text{dec}}, t_{\text{com}}, t_{\text{disp}}$and the aggregate indicator T_{info}. This decomposition enables quantitative attribution of delay to validation, decision authorization, and directive dissemination, which is critical for airbases characterized by dense legitimate activity and high alarm load.

New, domain-specific regularities are systematized for the aviation protection context: the dominant mechanisms that erode sufficiency arise from growth of validation and decision latency under signal ambiguity, concurrent incidents, and communications degradation, as well as from reduced resilience to false-alarm surges. These findings clarify the previously under-specified role of information processes as a limiting factor for airbase physical protection.

The paper introduces practical artifacts suitable for conceptual design and review, including an airbase scenario matrix that identifies dominant information bottlenecks and preferred acceptance evidence channels, and an information-to-action metric catalogue with target types (upper bounds on time, lower bounds on probability and availability, and limits on false-alarm rate and workload). Together, these artifacts provide a quantitative bridge from threat scenarios to verifiable requirement statements.

A verification approach is substantiated to support evidential credibility and acceptance, combining instrumented timed drills, log-based measurement, stress tests (alarm-load and degraded-communications conditions), and simulation or hybrid evidence for rare multi-event regimes. This approach strengthens reproducibility of latency measurements and reduces the risk of "documented compliance without operational sufficiency."

The practical significance of the results lies in enabling airbase and airfield protection programs to (i) specify measurable latency and information-quality targets, (ii) identify and mitigate bottlenecks in validation, decision-making, and communications, (iii) establish audit-ready acceptance evidence, and (iv) implement lifecycle revalidation using operational logs and after-action review. This supports improved resilience to time-compressed and concurrent threat conditions and provides a defensible basis for modernization prioritization and resource allocation.

REFERENCES

1. Yang, J., Huang, L., Ma, H., Xu, Z., Yang, M., & Guo, S. (2022). A 2D-graph model-based heuristic approach to visual backtracking security vulnerabilities in physical protection systems. International Journal of Critical Infrastructure Protection, 38, 100554. DOI: https://doi.org/10.1016/j.ijcip.2022.100554.
2. Akhundov, R., & Hashimov, E. (2025, November). Enhancing the efficiency of the military environmental security system through the implementation of advanced technical means. In Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference (No. 8, pp. 348–352).
3. Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk Analysis, 1(1), 11–27. DOI: https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.
4. Islamov, I. et al. (2025). Hybrid communication models for UAV swarms: Towards scalable and energy-aware network optimization. Scientific guidelines: Theory and practice of research – Proceedings of the VI International Scientific Conference (Kyiv, Ukraine, October 3, 2025), pp. 185–195. DOI: https://doi.org/10.62731/mcnd-03.10.2025.
5. Garcia, M. L. Design and Evaluation of Physical Protection Systems. 2nd ed. Elsevier, 2008. DOI: https://doi.org/10.1016/C2009-0-25612-1.
6. Hashimov, E., Akhundov, R. G., Talibov, A. M., & Islamov, I. (2026). Constrained optimization of an integral security indicator for adaptive management of hazardous facilities. Grail of Science, (62), 1003–1014. DOI: https://doi.org/10.36074/grail-of-science.20.02.2026.109.
7. Cozens, P., & Love, T. (2015). A Review and Current Status of Crime Prevention through Environmental Design (CPTED). Journal of Planning Literature, 30(4), 393–412. DOI: https://doi.org/10.1177/0885412215595440.
8. Talibov, A. M., Hashimov, E. G., & Akhundov, R. G. (2025). Modeling and forecasting radiological and chemical threats in the military sphere. In Current directions of development of information and communication technologies and control tools: Proceedings of the 15th International Scientific and Technical Conference (Vol. 1, pp. 120–121).
9. Akhundov, R., Hashimov, E. G., & Islamov, I. (2026). Conceptual models of multi-level physical protection systems for special-purpose and critical infrastructure facilities. Grail of Science, (61), 591–608. DOI: https://doi.org/10.36074/grail-of-science.23.01.2026.066.
10. Rehak, D., Slivkova, S., Janeckova, H., Stuberova, D., & Hromada, M. (2022). Strengthening Resilience in the Energy Critical Infrastructure: Methodological

Overview. Energies, 15(14), 5276. DOI: https://doi.org/10.3390/en15145276.
11. Islamov, I. et al. (2025). Big data analytics and machine learning for predicting radiation and chemical threats in the military sphere. Theory and practice of modern science: Collection of scientific papers «SCIENTIA» with proceedings of the X International Scientific and Theoretical Conference (September 26, 2025, Kraków, Republic of Poland) (pp. 30–38). DOI: https://doi.org/10.36074/scientia-26.09.2025.
12. Lovecek, T., Ristvej, J., & Simak, L. (2010). Critical Infrastructure Protection Systems Effectiveness Evaluation. Journal of Homeland Security and Emergency Management, 7(1). DOI: https://doi.org/10.2202/1547-7355.1613/.
13. Akhundov, R., & Hashimov, E. (2026). Enhancing the physical protection of critical facilities through the integration of physical process models and machine learning. Grail of Science, (61), 722–731. DOI: https://doi.org/10.36074/grail-of-science.23.01.2026.083.
14. Mondal, S., Adak, B., & Mukhopadhyay, S. (2023). Functional and smart textiles for military and defence applications. In Smart and functional textiles (p. 397).
15. Shoop, B., et al. (2006). Mobile detection assessment and response systems (MDARS): A force protection physical security operational success. In Unmanned Systems Technology VIII (Vol. 6230, pp. 68–678). SPIE.
16. Hashimov, E., Akhundov, R., Talibov, A., & Islamov, I. (2026). Decision support for physical protection systems using route-level metrics and simulation-based evaluation. Grail of Science, (63), 531–542. DOI: https://doi.org/10.36074/grail-of-science.06.03.2026.059.
17. Kampova, K., Lovecek, T., & Řehák, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. International Journal of Critical Infrastructure Protection, 30, 100376. DOI: https://doi.org/10.1016/j.ijcip.2020.100376.
18. Zou, B., Yang, M., Zhang, Y., Benjamin, E.-R., Tan, K., Wu, W., & Yoshikawa, H. (2018). Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant. International Journal of Critical Infrastructure Protection, 23, 90–99. DOI: https://doi.org/10.1016/j.ijcip.2018.08.006.
19. Islamov, I. et al. (2025). Innovative approaches to environmental recovery in conflict-affected areas. In Scientific discoveries and fundamental research: World experience: Proceedings of the VII International Scientific Conference (pp. 180–190). Zhytomyr, Ukraine: Ukrlogos Group. DOI: https://doi.org/10.62731/mcnd-24.10.2025.
20. Akhundov, R., Hashimov, E. G., & Islamov, I. (2026). Methodological limitations of normative design of physical protection systems for critical and military facilities in a dynamic threat environment. International scientific journal «Grail of Science», (62), 873–889.
21. Řehák, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. International Journal of Critical Infrastructure Protection, 25, 125–138. DOI: https://doi.org/10.1016/j.ijcip.2019.03.003.
22. El Wely, I. C., Chetaine A. (2020). Analysis of physical protection system effectiveness of nuclear power plants based on performance approach. Annals of Nuclear Energy, 153, 108051. DOI: https://doi.org/10.1016/j.anucene.2020.107980.
23. Islamov, I. et al. (2025). The use of unmanned systems and artificial intelligence to enhance radiation and chemical safety in military ecology. In Innovations and the scientific potential of the world: Proceedings of the VII International Scientific Conference (pp. 183–192). DOI: https://doi.org/10.62731/mcnd-10.10.2025.
24. Akhundov, R., & Islamov, I. (2025, November). Military Environmental Security under Radiation and Chemical Threats. In Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference (No. 8, pp. 414 –419).
25. Genserik L.L. Reniers, Amaryllis Audenaert (2014). Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Safety and Environmental Protection, 92(6), 583–589. DOI: https://doi.org/10.1016/j.psep.2013.04.002.
26. Hashimov, E. et al. (2026). Research of the efficıency multıservıce networks usıng MIMO technology. Advanced Information Systems, 10(1), 66-71. DOI: https://doi.org/10.20998/2522-9052.2026.1.08.
27. Islamov, I. et al. (2025). Integrating environmental security into defense strategy with a focus on radiological and chemical risks. Strategic directions of science development: Factors of influence and interaction: Collection of scientific papers with materials of the VII International Scientific Conference (September 26, 2025, Cherkasy, Ukraine) (pp. 115–125). DOI: https://doi.org/10.62731/mcnd-26.09.2025.
28. Akhundov, R., & Hashimov, E. G. (2025). Quantitative categorization of facilities and modeling of potential adversaries. Grail of Science, (60), 469–482. DOI: https://doi.org/10.36074/grail-of-science.26.12.2025.049.
29. Islamov, I. et al. (2025). Controller-level scalability problems in software-defined networks. In Problems of Informatization: Proceedings of the 13th International Scientific and Technical Conference (Vol. 1, pp. 70–71).
30. Akhundov, R., Hashimov, E. G., & Islamov, I. (2026). Scenario oriented sufficiency criteria for physical protection systems provide a traceable path from threat classes to design requirements. Grail of Science, (63). DOI: https://doi.org/10.36074/grail-of-science.06.03.2026.074.

31. Islamov, I. et al. (2025). Prospects for the use of robotic complexes in eliminating the consequences of environmental accidents at military facilities. In Achievements and advancements of applied and fundamental sciences of the 21st century: Proceedings of the X International Scientific Conference (pp. 301–311). Dnipro, Ukraine: Ukrlogos Group. DOI: https://doi.org/10.62731/mcnd-07.11.2025

The article has been submitted to the editorial office 20.03.2026

Вимоги до інформаційно-допоміжних дій для фізичного захисту авіабази в умовах високотемпових атак противника

Анотація

У дослідженні розглядаються інформаційні процеси, які відбуваються під час фізичного захисту авіабаз та аеродромів, коли вони функціонують в умовах інтенсивного протистояння противника. При цьому легітимна щільна активність противника збільшує неоднозначність щодо прийняття рішень та створює велике навантаження. У статті основна увага приділяється ефективності перетворення інформації на дію як критичному фактору достатності, що пов’язує сенсорне спостереження з перевіркою рішень, їх відправкою та активацією реагування в межах часового вікна, що дає змогу перервати роботу до того, як зловмисник досягне критичного елемента.

Мета полягає в тому, щоб визначити вимірні вимоги до інформації для реагування на авіаційні об’єкти, які залишаються захищеними за умов паралельної роботи, сплесків хибної тривоги, погіршення зв’язку та впливу внутрішніх осіб.

Методологія поєднує бібліотеку обмежених сценаріїв з розкладанням затримки на складові, ідентифікацію вузьких місць для кожного класу сценарію та обґрунтування вимог до часових обмежень та цільових показників якості. Прийняття рішення визначається за допомогою попередньо визначених каналів доказів, включаючи інструментальні тренування з фіксованим часом, аналіз журналів SOC та C2, стрес-тести для сигнального навантаження та погіршення зв’язку, а також моделювання. Для рідкісних режимів з кількома подіями використовуються гібридні докази. Інтерпретація результатів включає матрицю сценаріїв функціонування авіабази, що відображає:

домінантні інформаційні вузькі місця на шляхах перевірки;

каталог метрик з типами цілей для затримки, якості виявлення та класифікації, стійкості до хибних тривог та доступності зв’язку.

Аналіз результатів показує, що зниження достатності насамперед зумовлене зростанням затримки перевірки та прийняття рішень в умовах неоднозначності та перевантаження, а не лише наявністю датчиків.

Наведений підхід застосовується до концептуального проєктування, специфікацій закупівель для робочих процесів SOC та C2, програм приймального тестування та повторної валідації життєвого циклу з використанням операційних журналів та перевірки після дій.

Ключові слова: безпека авіабази; система фізичного захисту; затримка від інформації до дії; перевірка тривоги, затримка прийняття рішень; командування та управління; стійкість зв'язку; сценарні вимоги; підтвердження прийнятності.